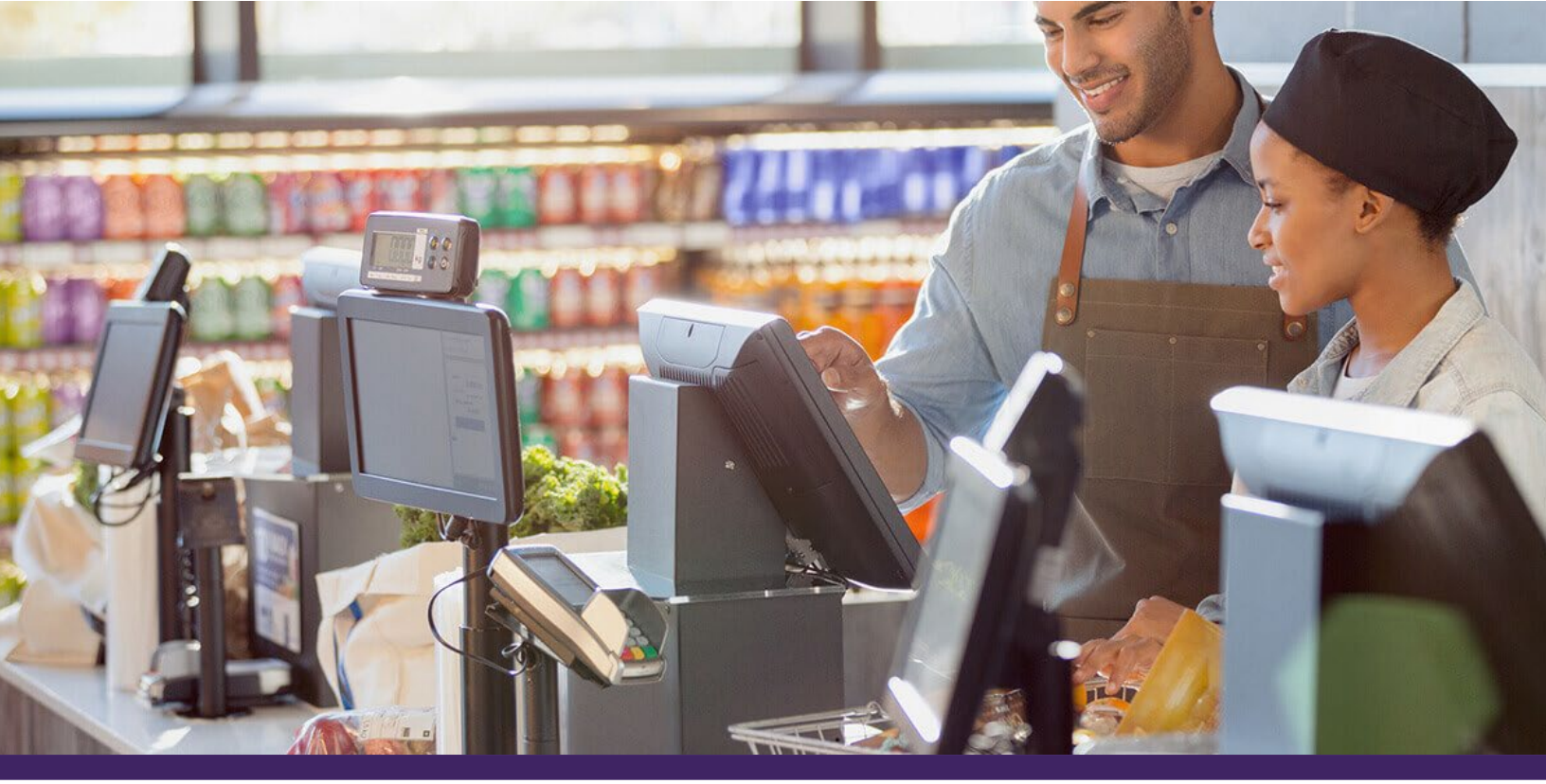
AGENTLESS DEVICE SECURITY FOR RETAIL ENVIRONMENTS


ed Deli
bossanova

TABLE OF CONTENTS



EXECUTIVE SUMMARY

As a retailer, digitally transforming your brick-and-mortar stores can grow revenue, reduce costs, and deliver new, exciting shopping experiences that attract and retain customers. However, the connected devices that make digital transformation possible can also put your business at risk.

The connected devices that make digital transformation possible are, more often than not, unmanaged, meaning they are not seen or controlled by your security or IT teams. That's because many of these unmanaged devices can't host a security agent, leaving your security team blind to what the devices are doing. So increasingly, cybercriminals focus on these devices as targets because of their ubiquity and inherent security weaknesses.

The digital transformation to using modern, connected retail devices shouldn't come at the cost of incurring unacceptable levels of cyber risk. Deployments of devices like these require security that's purpose-built for today's connected, unmanaged devices, and that includes continuous device monitoring that detects threats and responds automatically to mitigate risk.

This white paper explores the cyber security challenges in retail environments and propose ways to address them.

THE CONNECTED RETAIL AGE IS HERE

Smart, connected devices, often referred to as the Internet of Things (IoT), present an opportunity to develop a retail shopping environment that connects the physical and digital worlds, enabling real-time interaction with consumers.

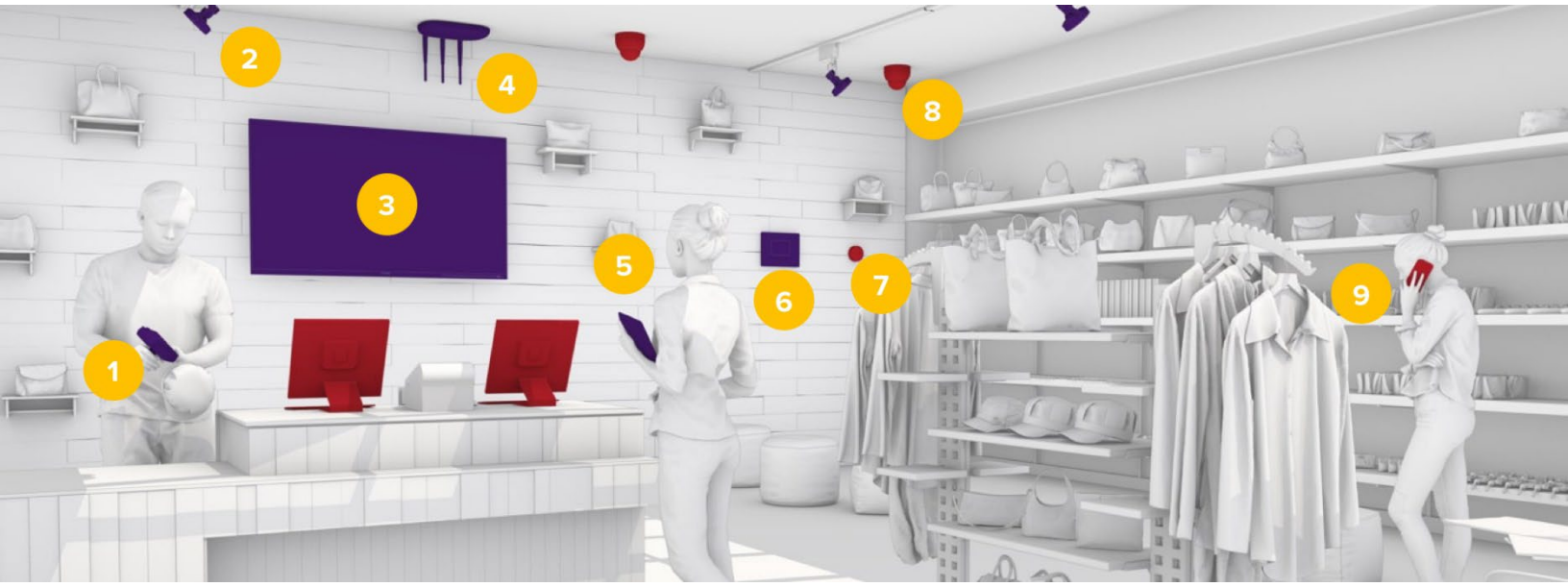
Visionary retailers are thinking years ahead about how to leverage not only this technology, but also artificial intelligence, machine learning, and autonomous robotics to improve marketing and operational efficiencies. Retailers are also using these devices in innovative ways that improve the shopping experience:

- As shoppers enter a store, the store's Wi-Fi network can send notifications to shoppers' smartphones and devices with targeted messages and coupons for products similar to what they've bought before.
- Sensors can track customers' paths through a store, and you can use the tracking information to improve layout and merchandise placement.
- Interactive kiosks and smart displays can provide store layouts, directions, and product information.
- Automated inventory systems that include devices like robots that continuously scan store floors for restocking needs and for general orderliness of shelves or displays.
- Self-service checkout can help customers complete the purchase process more quickly.
- Facial recognition can identify known shoplifters or can identify customers and inform salespeople about preferences like colors and sizes.
- Open Wi-Fi keeps customers connected while organizations gain critical information about movement, location, shopping habits, and conversions.

These innovations capitalize on customer's preferences for personalized experiences and engagement. However, they also depend on devices that can be a big security risk. These devices expose an increasingly vulnerable attack surface because they can't be updated easily and they aren't monitored for potential compromises.

THE AGE OF THE UNMANAGED DEVICE

This new age of connected retail also brings in a new age of unmanaged devices driving that transformation. From smart displays and customer sensors to mobile point of sale devices to inventory robots in a store to internet connected forklifts unloading new goods, each of these devices are the new endpoint. However, these new endpoints do not come with security, nor can they host an agent. In fact, many are un-agentable. This means the very devices used to drive connection, productivity, and interaction do not have the level of protection security professionals are used or required for endpoints in their environments.



1 **Barcode Scanners**
May use Bluetooth or Wi-Fi. Hard to patch, but remotely exploitable.

2 **Smart Lighting**
On the network with no security.

3 **Smart TV**
Can't take an agent, but on the network. Hard to upgrade.

4 **Point of Sale**
Tablets & handheld devices. Taking credit cards and digital payments.

5 **Tablets**
Used for mobile Point of Sale, inventory lookup, support, and more.

6 **Security Systems**
On the network, but security on these devices is questionable.

7 **Smart HVAC**
Smart HVACs and thermostats can't take agents.

8 **Security Camera**
No security, but often the target of botnets and other attacks.

9 **Smartphone**
Transient devices used by customers and vendors. Should identify and track.

SECURITY BREACHES ARE COMMON

Security breaches at U.S. retail stores are on the rise. Breaches more than doubled in 2017 and included nearly half of all stores in 2018.[1] For perspective, retail was the second most breached industry, only slightly trailing the U.S. federal government, and ranking ahead of both the healthcare and financial services industries.

For one example, the Hudson's Bay data breaches involving malicious code on infected registers at Saks Fifth Avenue, Saks Off 5th, and Lord & Taylor stores went on *for months* before they were stopped.[2] Over five million credit and debit card numbers were stolen — a shocking breach, but certainly not the biggest we're likely to see, or the most expensive.

---

1 U.S. retail data breaches more than doubled according to the Thales report, rising to 50% in 2018 from 19% in a 2017 survey. (Jul 2018)

2 Card Data Stolen From 5 Million Saks and Lord & Taylor Customers, New York Times, Apr. 1, 2018.

These are just the exposures we know about. More likely is the case that breaches occur every day that we don't know about — until we do. That's because vulnerabilities in devices are far more elusive to retailers than they are to bad actors. And it only takes one vulnerability to put an entire business at risk.

These unmanaged and IoT devices are the new targets for hackers. New research[3] shows cyberattacks on IoT devices surged 300%, targeted billions of devices across multiple industries including retail. The lack of any security on these unmanaged and IoT devices makes them the new attack landscape for bad actors.

SECURITY BREACHES ARE COSTLY

The bigger the breach, the more costly it is due to the added resources needed to recover from the breach and the cost of lost business following public disclosure. Eddie Bauer is facing a $9.8M tab for a data breach,[4] and Neiman Marcus not only had to pay a $1.5 million settlement[5] but was also required to implement new security procedures.

Perhaps the most high profile data breach in recent memory was Target in 2013, which resulted in an $18.5 million settlement.[6] But the overall cost was much higher. Target also paid $10 million to settle a class-action lawsuit in 2015, and the company agreed to pay up to $10,000 to consumers who suffered losses from the data breach. With a loss of customers in the first few quarters following the breach, the total cost was an estimated $300 million as of mid-2017.[7]

The bottom line is that aside from expensive downtime and breach recovery, retailers today have to concern themselves with regulators that could impose heavy fines on top of lost revenue and diminished customer trust.

---

3 Forbes, Cyberattacks On IOT Devices Surge 300% In 2019, 'Measured In Billions', Report Claims, Sept. 2019

4 According to the filing, outdoor apparel retailer will pay up to $2.8 million in settlement distributions, $2 million to cover attorney fees and other costs, and about $5 million taking steps to ensure that its payment and cybersecurity systems are safe. (May 2019)

5 Neiman Marcus paid a $1.5 million settlement for a breach of over 370,000 credit cards, and as part of the settlement, the company is required to implement new procedures to protect customers' personal information and ward off future attacks. (Jan. 2019)

6 "Target will pay $18.5 million in settlement with states over 2013 data breach", L.A. Times, May 23, 2017.

7 "The Supply Side: Walmart cybersecurity team handles over 200 billion events annually", Talk Business & Politics, May 22, 2019.

REGULATIONS LOOM OVER RETAILERS

Following critical security controls is a mainstay for any security professional. But following security frameworks such as NIST and CIS to properly secure unmanaged and IoT devices may not be enough. It's critical to deploy device security that can help you achieve compliance, otherwise companies that can't risk fines anywhere from $5,000 to $100,000 per month.

A retailer must comply with the Payment Card Industry Security Standard (PCI DSS) as they conduct their business. They must look at how they will meet these standards, documenting, monitoring, and enforcing policy on all devices in the cardholder data environment — including unmanaged or IoT devices beyond the reach of traditional controls such as endpoint security or network firewalls.

Compliance with SOX[8] is also vital for publicly traded retail companies. Regulators demand that companies pay strict attention to core risk management governance, controls, practices, and reporting — particularly in the areas of cybersecurity and third-party risk management. Non-compliance with SOX risks severe penalties, including fines of up to $5 million and prison time.

8 The Sarbanes-Oxley Act

REAL THREATS IN THE DIGITAL RETAIL ENVIRONMENT

- **Smart displays and kiosks:** Internet-connected devices can be attacked remotely to give attackers access to your network.
- **Self-serve checkout and point-of-sale (POS) devices:** Theft of shopper credit/debit card information costs time and expense to fix but also causes millions in regulatory fines and damage to your brand.
- **Bluetooth-enabled price scanners:** Hackers can attack these devices through Bluetooth-related vulnerabilities to change the pricing of items or stage a broader attack for customer information.
- **Printers connected to Wi-Fi:** A printer with an open hotspot can enable hackers to circumvent network access control and gain access to your data.
- **Production-line sensors:** Sensors and automated controls in warehouses can be compromised causing production or delivery delays.

TRADITIONAL SECURITY WASN'T BUILT FOR UNMANAGED AND IOT DEVICES

In the rush toward digital transformation, the primary focus has been to acquire and deploy digital retail devices at scale to quickly reap their rewards—like helping to grow revenue, reducing costs, gathering critical data, and delivering new shopping experiences. Security has not been a front-and-center concern. These devices are designed to connect, and some actively seek connections whether you want them to or not. Once these devices are on your network, their vulnerabilities become a risk you have to face.

The traditional security products most organizations have come to know and trust simply won't help manage the risks and consequences of the new connected retail frontier. These products were built for traditional computing devices. And while some security vendors have reengineered their products, or have offered new bolt-on modules that attempt to make them work for IoT and unmanaged devices, most fail for a variety of reasons:

- **Security agents won't work.** You cannot install an agent on most retail unmanaged and IoT devices. This renders invalid an entire class of security tools that are often used to help identify, protect and monitor devices on enterprise networks.
- **Network scanners can't be used.** Many of these devices do not tolerate network scans or probes, which can crash or disrupt the device. That makes obtaining an inventory of hardware, software, and vulnerabilities are far more challenging for IoT devices than for normal computers.
- **Conventional network security products are insufficient.** The traditional placement of network IPS systems is at the perimeter and in the core of the network. This makes protecting IoT devices at the edge of the network difficult or impossible. Furthermore, network equipment can be compromised by a determined hacker, so relying exclusively on network controls (e.g. firewalls and network segmentation) is unwise.

- **Wireless connectivity evades legacy security controls.** Manufacturers of network devices like access points and routers as well as OT security products are increasingly building wireless connectivity into their devices. These protocols, which include Bluetooth, Near Field Communication, Zigbee, etc. are invisible to traditional security controls.

FUNCTIONAL GAPS IN TRADITIONAL SECURITY PRODUCTS

No visibility

Visibility is an essential component of any security strategy. However, traditional security products can't adequately see or monitor the "smart" devices that are used in most digital transformation projects. Nor can they see or monitor devices that employees bring into the store without your knowledge. Inventory tools that claim to provide "visibility" or "discovery" were not designed to discover or assess these unmanaged assets or IoT devices. As a result, you're left with an incomplete picture of the devices and risks in your environment.

This is a huge security problem. Bad actors target common IoT devices like VoIP phones, smart TVs, IP cameras and more to gain a foothold into the network, and then branch out deeper into more lucrative areas - like payment networks. This makes discovering and classifying every managed, unmanaged, and IoT device in your environment vital.

Having critical information about devices including manufacturer, model, serial number, location, username, operating system, installed applications, and connections made over time can help determine exactly what device is exhibiting suspicious behavior, and how it's interacting with your network. It also makes it easier to track the connection and activity history of every device in the environment with granularity.

No risk assessment

Identifying risks is a critical part of any retailer's security strategy. You need to assess risk based on a variety of factors like vulnerabilities, known attack patterns, and the behaviors observed of each device on your network. This information is needed in order to understand your attack surface and to comply with regulatory frameworks that require identification and prioritization of vulnerabilities. However, traditional vulnerability scanner products that run periodically (weekly or monthly) can miss transient devices, like those employees and customers bring into the environment, and they can even knock some devices off-line altogether.

No threat detection

The most common way to detect threats is to monitor an endpoint using a security agent. But you can't put an agent on these devices, which renders them invisible to traditional threat detection products. That lack of coverage makes these devices highly vulnerable to threats. Retailers need agentless threat detection that can detect activities with these devices, including changes in device state and anomalies reported about similar devices. You also need to automate your threat response and quarantine devices automatically.

MITIGATING SECURITY RISKS

Since traditional security tools are unable to monitor and secure unmanaged retail and IoT devices, security professionals must seek a new approach. This new way forward in security must be purpose-built for today's unmanaged, connected environments. That includes the ability to discover all the devices in remote locations, proactively assess the risk of every device, and detect threats by monitoring and analyzing device behavior continuously. And it must be able to respond to incidents immediately and automatically to stop attacks from unraveling your business.

An Agentless Approach

As previously discussed, several security products use proprietary software agents and even additional hardware to scan devices for information. For managed devices, agent-based tools can provide detailed information — but only when the agents are working properly. More importantly, the scope of agent-based products does not extend to unmanaged or IoT devices.

Armis is designed to address unmanaged and IoT devices using an agentless approach. Without installing or licensing separate software or hardware, Armis can see every device in your organization, managed and unmanaged, and the connections those devices make. With no agents to deploy or manage, it works equally well for any unmanaged and IoT devices. And it is completely passive, so as not to disrupt the operation of any device in your retail operations.

Armis is cloud-based and integrates easily with your existing network and security products — nothing to install on devices, and no configuration or programming required. It integrates with your existing enforcement points like firewalls and NAC, and enables you to create fine-grained policies for unmanaged and IoT devices to extend the value of your security investments.

Discover devices other products miss

The right device security product should discover every device on and off your network, and analyze their behavior, including connections and activity history. Specifically, you need a security solution that can monitor both wired and wireless traffic on your network and in your airspace to identify every device and to understand their behaviors.

Armis can detect, classify, and profile every managed, unmanaged, and IoT device in your environment, giving you a complete, real-time device inventory and an unprecedented level of visibility and control. Armis can even identify off-network devices using Wi-Fi, Bluetooth, and other IoT protocols in your environment — a capability no other security product offers without adding additional hardware.

Assess the risk of attack surfaces

Investing in risk assessments can help you manage your organization's attack surface and enable you to pinpoint risky devices and activities. Armis provides modern retailers with ongoing device risk scoring based on multiple risk factors, including software vulnerabilities, known attack patterns, and the behaviors that Armis observes of each device on your network. The risk score helps your security team understand your attack surface and meet compliance with regulatory frameworks that require identification and prioritization of vulnerabilities.

Detect threats with continuous monitoring

Continuous monitoring is essential for maintaining security with unmanaged and IoT devices. Core to the Armis platform is our Device Knowledgebase. It is a giant, crowd-sourced, cloud-based device behavior knowledgebase—the largest in the world. It tracks 110 million devices broken out into 10 million distinct device profiles. These device insights enable Armis to classify devices and detect threats with a high degree of accuracy.

Armis compares real-time device state and behavior to “known-good” baselines to similar devices we have seen other environments. Using it’s unique threat detection and prevention technology, Armis can detect changes in device states and anomalies that could indicate threats or attacks and can automate threat response. Armis continuously monitors every device on your network to detect suspicious or malicious activity and automatically quarantines suspicious devices to stop attacks and any exposure to the rest of your business.

Stop attacks instantly and automatically

Visibility and continuous monitoring are not enough. You need to take action and quarantine suspicious or malicious devices. When Armis detects a threat, it can alert your security team and trigger automated actions to stop an attack. This automation helps reduce security team workload by creating policies that mitigate and alert on critical events automatically.

Armis integrates with your switches and wireless LAN controllers, as well as with your existing security enforcement points like Cisco and Palo Alto Networks firewalls, and NAC products such as Cisco ISE and Aruba ClearPass. This automation and integration provide peace of mind that an attack on any device — managed or unmanaged — will be stopped, even if your security team is busy with other priorities.

Integration Without Disruption

Frictionless integration — without disruption in your environment — is the key to successful deployment. You want security products that install in minutes and use the infrastructure you already have, with no impact on your organization’s network performance. Armis integrates with your existing infrastructure, including NAC, firewall, SIEM, CMDB, and more.

CONCLUSION

The digital transformation in retail is already underway, as businesses look to find new ways to engage with customers while simultaneously driving productivity, operational efficiency, and sales. That transformation comes with a new generation of connected devices - unmanaged and IoT devices designed to connect, but with no inherent security.

With attacks on unmanaged and IoT devices on the rise, and many high-profile vulnerabilities making headlines, security professionals know the time to act is now. This transformation of retail places thousands of unmanaged devices in your store and on your network at any given time. Those new security risks are real, especially with the advent of connected unmanaged and IoT devices. Designed to connect in an increasingly wireless world, IoT devices are not built with security in mind. Cybercriminals are already exploiting that fact.

Armis is the first agentless, enterprise-class security platform to address the new threat landscape of unmanaged and IoT devices. Armis fills a massive gap, providing agentless security from the warehouse to the shelf and checkout aisle for the growing number of unmanaged devices in modern retail. Armis security helps you fulfill the promise of the future of digital retail: to conduct business, attract customers, and manage resources faster and more efficiently.

ABOUT ARMIS

Armis is the first agentless, enterprise-class security platform to address the new threat landscape of unmanaged and IoT devices. Fortune 1000 companies trust our unique out-of-band sensing technology to discover and analyze all managed, unmanaged, and IoT devices – from traditional devices like laptop and smartphones to new unmanaged smart devices like smart TVs, webcams, printers, HVAC systems, industrial robots, IoT devices and more. Armis discovers devices on and off the network, continuously analyzes endpoint behavior to identify risks and attacks, and protects critical information and systems by identifying suspicious or malicious devices and quarantining them. Armis is a privately held company and headquartered in Palo Alto, California.

20190919-1

1.888.452.4011
armis.com